VMware vSphere Data Protection

Replication Target

TECHNICAL WHITEPAPER

Table of Contents

Executive Summary

This technical white paper introduces the vSphere Data Protection Replication Target identity. It also provides an overview of replication in vSphere Data Protection and documents the best practices and use cases for building a backup data replication strategy using VDP Advanced.

VDP Identities

vSphere Data Protection 5.8 comes with three identities or editions that can be deployed:

vSphere Data Protection (VDP):

This is the default identity, which includes basic capabilities such as backup and restore of virtual machines using vStorage APIs for Data Protection (VADP). It also includes ability to recover individual VM files. VDP can replicate only to EMC Avamar. VDP cannot replicate to other VDP appliances.

vSphere Data Protection Advanced (VDP Advanced) :

This identity comes with set of extended features, which are license based. Additional features in VDP Advanced include increased backup data storage capacity, ability to replicate backup data to another VDP Advanced or VDP Replication Target appliance, support for application consistent backups, and support for EMC Data Domain as backup storage. For a full list of features available in VDP Advanced, please refer to the vSphere Data Protection 5.8 administration guide.

vSphere Data Protection Replication Target (VDP-RT):

This identity comes with a unique capability, which allows the appliance to serve as a replication target for backup data from a source VDP Advanced or VDP-RT appliance. This identity does not require a license key. A VDP-RT appliance can perform restores from replicated backup data. Backup capabilities are disabled in a VDP-RT appliance.

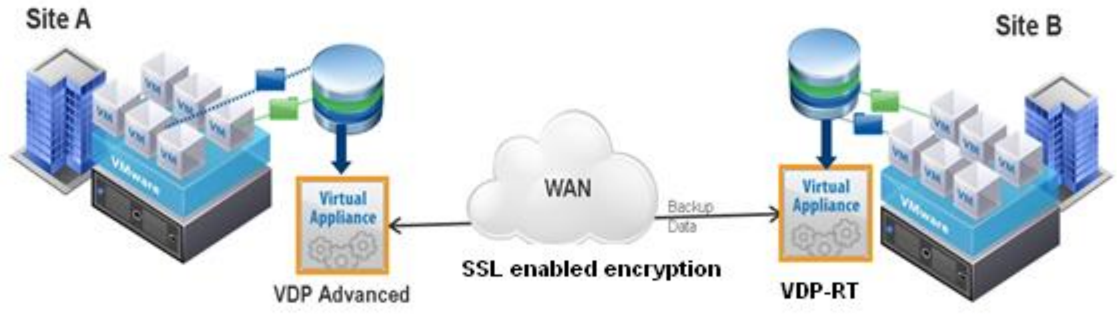
vSphere Data Protection Replication Target Identity (VDP-RT)

vSphere Data Protection Replication Target identity (VDP-RT) is a new feature introduced with the VDP 5.8 release. VDP-RT is deployed similar to other VDP appliance identities. VDP-RT provides backup administrators a backup data replication target for VDP Advanced and other VDP-RT appliance(s).

Some of the key characteristics and benefits of the VDP-RT identity are as follows:

- Provides a simple, efficient and secure way to replicate backup data within a data center and across data centers.
- In the event of a disaster where a VDP Advanced appliance becomes unavailable, data can be recovered directly from the replication target, providing high level of availability.
- In case of a failed upgrade, where a VDP Advanced appliance has lost all the latest backups and has rolled back to a safe state, the VDP-RT can recover replicated clients.
- Replication can be performed in a cascading manner to provide multiple end points for replicated backups. Replication from one VDP-RT to another VDP-RT is supported.
- VDP-RT does not have a backup window. Replicated backup data can be received by a VDP-RT appliance at any time.
- No license is required to deploy a VDP-RT appliance. There is no longer a need for a zero-CPU “replication target only” license key as was the case with VDP Advanced 5.5.
- VDP-RT can be upgraded to a VDP Advanced appliance anytime with a valid license key.
- Backup data can be replicated to multiple VDP-RT appliances, i.e. one to many, thus providing multiple end points for protection of its backup clients.
- VDP-RT appliance with a Data Domain system configured can act as a replication target for any VDP Advanced having a Data Domain system configured. Note that if backup data in the source appliance is stored on a Data Domain system then the target appliance for replication must also have a Data Domain system configured.
- Multi-tenancy support provides tenants the flexibility to manage their own set of backups within a namespace.
- Backup data capacity expansion is supported in VDP-RT similar to VDP Advanced.
- Replication will still continue to work even if vCenter server at either source or destination goes offline.
- Emergency restore is fully supported with VDP-RT, allowing user to perform image level restores even if the vCenter Server connected to the target appliance is offline.

Replication in VDP

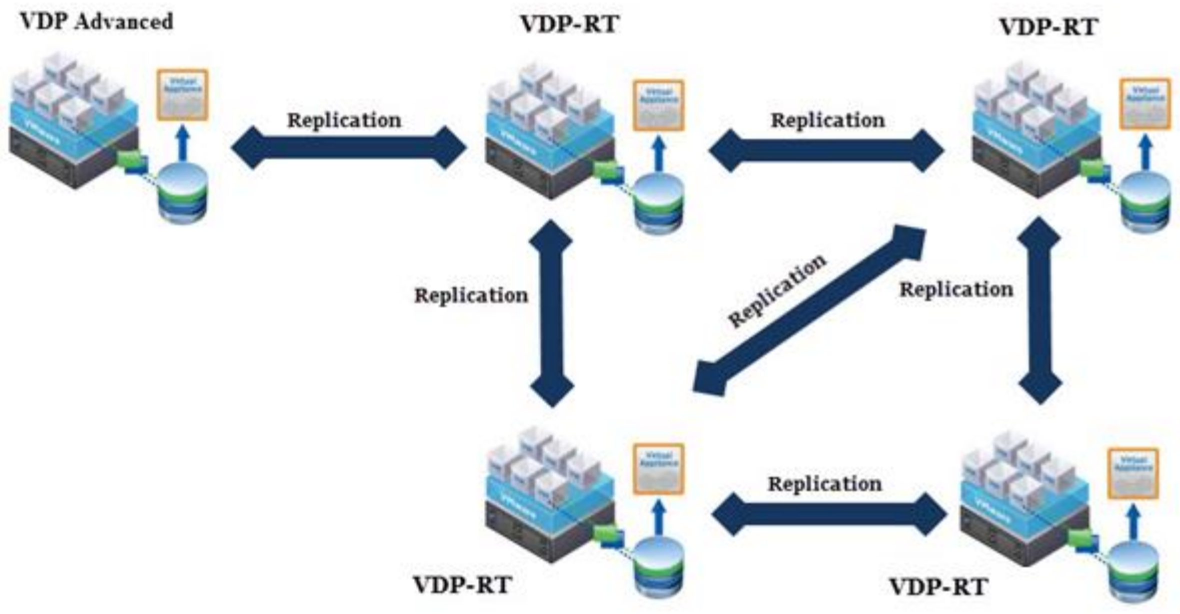


VDP replication is a feature that enables efficient, encrypted, asynchronous replication of backup data stored in an VDP Advanced appliance to another VDP Advanced or VDP-RT appliance deployed in remote locations without the need to ship tapes. Replication is a scheduled process between two independent appliances, providing a higher level of reliability for stored backups. Replication can be scheduled to run at off-peak hours to minimize bandwidth impact.

VDP replication is unique in that it sends only incremental and unique data segments over the network in SSL enabled encrypted format. VDP replication transmits, using Internet Protocol, only the new data segments that the target VDP appliance does not contain. Hence, WAN-optimized replication is built-in to the product. Over a period of time, as more data is replicated to the destination VDP appliance, greater commonality and decreased transfer times for replication will be realized. The backup data is always compressed and encrypted during flight in the replication cycle, which provides added security to the data.

With the capability of VDP-RT appliance identity, VDP takes the approach of allowing replication of backup data to a secondary virtual appliance for disaster recovery objectives without any additional licensing cost associated to the offsite appliance. Replication streams are WAN-optimized (minimum possible bandwidth requirements) and secure (encrypted).

Replication target topology overview



The replication topology diagram shown above illustrates how VDP-RT can be used to act as either a source or target of replication. As shown in the above diagram, replication is supported in fan-in topology, i.e. multiple sources to single target and fan-out topology, i.e. single source to multiple target topologies. Also cascading replication topology i.e. multiple hop topology can be implemented very easily using VDP-RT appliance at each hop.

The source appliance must be VDP Advanced for replication to work. The source backup data from the VDP Advanced appliance can be full image backups, individual disk backups, and/or application backups.

The recommended topology for deployment would depend on following factors:

- How many VDP Advanced appliances are deployed?
- How many tiers of protection to provide for backup data?
- How many offsite copies are required to be kept?

If there is only one VDP Advanced appliance deployed and one offsite copy has to be maintained at all time, then the recommended topology would be a source VDP Advanced replicating to one offsite VDP-RT appliance.

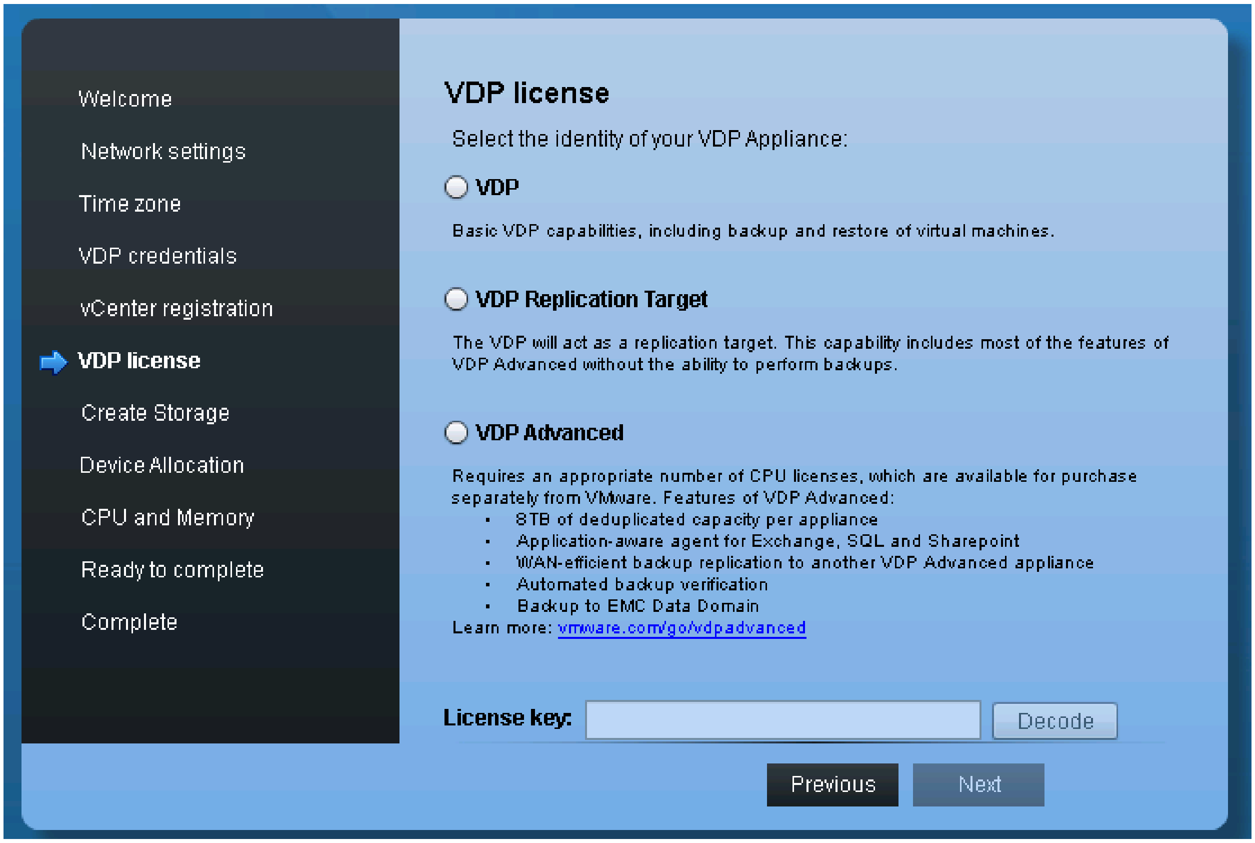
If there are multiple VDP Advanced appliances deployed and one offsite copy has to be maintained at all time, then the recommended topology would be multiple source VDP Advanced appliances replicating to single offsite VDP-RT appliance, i.e., a fan in topology

If there is single VDP Advanced appliances deployed and one offsite copy has to be maintained at all time with replication being directed to different locations dependent on the type of data, i.e. say all image backups are required to be stored at one offsite location while all application backups are required to be stored at another offsite location, then the recommended topology would be one source VDP Advanced replicating to multiple offsite VDP-RT appliances, i.e., a fan out topology

If there is single VDP Advanced appliances deployed and more than one offsite copy has to be maintained at all time with each copy having a different retention policy, then the recommended topology would be one source VDP Advanced replicating to offsite VDP-RT appliance 1 and VDP-RT appliance 1 replicating to offsite VDP-RT appliance 2, i.e., a cascading topology. Further levels of replication can be configured at each hop based on number of offsite copies required.

Deployment of VDP-RT

Deployment procedure for VDP-RT is similar to VDP-Advanced. The only difference is that no license key is required during VDP-RT deployment.



VDP license

Select the identity of your VDP Appliance:

○ VDP

Basic VDP capabilities, including backup and restore of virtual machines.

○ VDP Replication Target

The VDP will act as a replication target. This capability includes most of the features of VDP Advanced without the ability to perform backups.

○ VDP Advanced

Requires an appropriate number of CPU licenses, which are available for purchase separately from VMware. Features of VDP Advanced:

- 8TB of deduplicated capacity per appliance
- Application-aware agent for Exchange, SQL and Sharepoint
- WAN-efficient backup replication to another VDP Advanced appliance
- Automated backup verification
- Backup to EMC Data Domain

Learn more: vmware.com/go/vdpadvanced

License key:

Above screenshot shows the options seen during VDP deployment

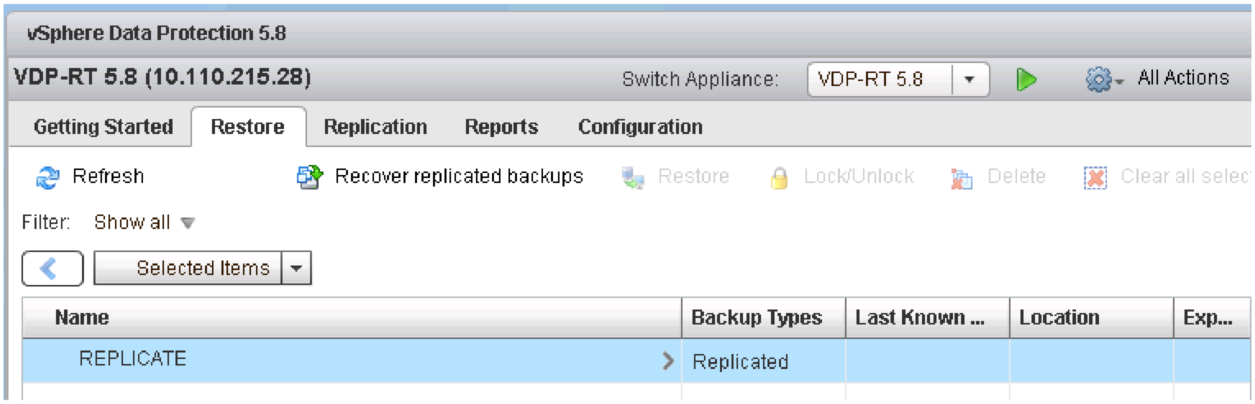
For complete details on how to deploy a new appliance, refer to *the vSphere Data Protection 5.8 Administration Guide*.

Accessing the replicated data

Under the Restore tab on a replication target (VDP Advanced or VDP-RT), a 'REPLICATE' link will be generated after successful replication from source to target. This link indicates that, this particular appliance is a target for either a source VDP Advanced or VDP-RT.

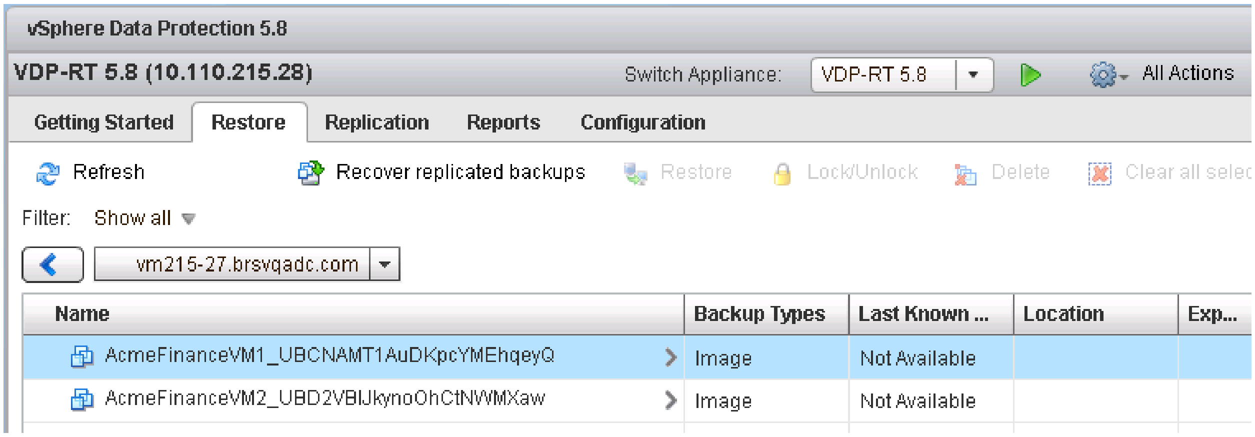
The 'REPLICATE' link when clicked on will expand and list out the hostnames of the source VDP Advanced or VDP-RT appliances. If the target appliance has multi-tenancy enabled, the 'REPLICATE' link can be expanded to the respective company and department names.

All the replicated data can be found under the respective source VDP Advanced or VDP-RT hostnames.



Name	Backup Types	Last Known ...	Location	Exp...
REPLICATE	Replicated			

'REPLICATE' link is shown above. Notice the Backup tab is missing from the VDP-RT appliance.



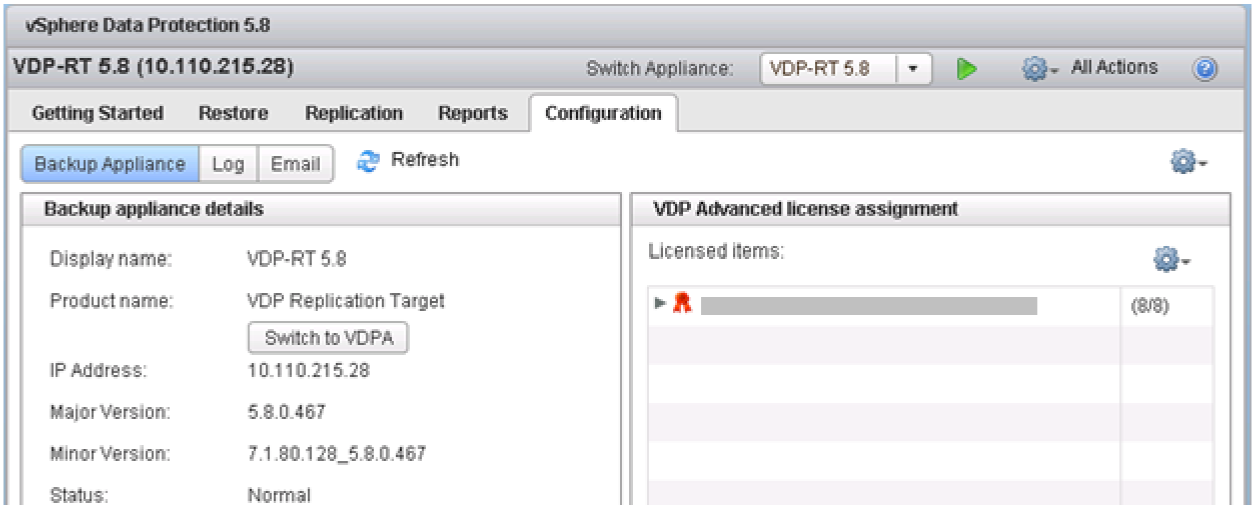
Name	Backup Types	Last Known ...	Location	Exp...
AcmeFinanceVM1_UBCNAMT1AuDKpcYMEhqeyQ	Image	Not Available		
AcmeFinanceVM2_UBD2VBIJkynoOhCtNWMXaw	Image	Not Available		

Expanding the 'REPLICATE' link will show the restore points listed under the source appliance hostname.

Switch identity from VDP-RT to VDP Advanced

VDP-RT can be switched to work as a VDP Advanced appliance at any given point in time by just adding a valid VDP Advanced license key using the Configuration tab of the VDP-RT appliance. After adding the license key and assigning the license to required set of hosts or clusters, one can click on "Switch to VDPA" button to complete the process. Post the switch, the appliance will work as any other VDP

Advanced appliance with all the extended features enabled. Do note that this is an irreversible process and one cannot switch back to VDP-RT mode post upgrade to VDP Advanced.



Display name: VDP-RT 5.8

Product name: VDP Replication Target

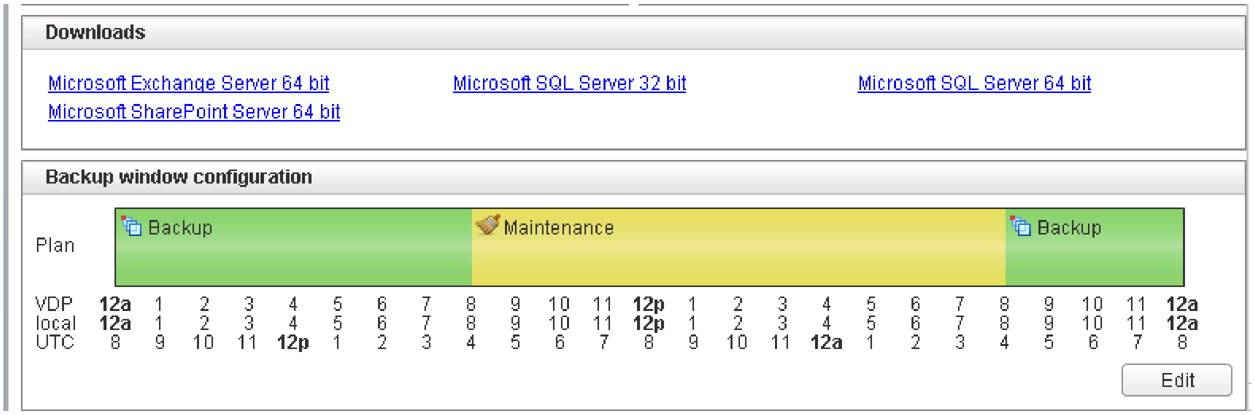
IP Address: 10.110.215.28

Major Version: 5.8.0.467

Minor Version: 7.1.80.128_5.8.0.467

Status: Normal

Above screenshot is of VDP-RT as seen before switch.


Downloads
Microsoft Exchange Server 64 bit
Microsoft SQL Server 32 bit
Microsoft SQL Server 64 bit
Microsoft SharePoint Server 64 bit
Backup window configuration
Plan
Backup
Maintenance
Backup
VDP 12a 1 2 3 4 5 6 7 8 9 10 11 12p 1 2 3 4 5 6 7 8 9 10 11 12a
local 12a 1 2 3 4 5 6 7 8 9 10 11 12p 1 2 3 4 5 6 7 8 9 10 11 12a
UTC 8 9 10 11 12p 1 2 3 4 5 6 7 8 9 10 11 12a 1 2 3 4 5 6 7 8
Edit

Above screenshot shows the backup window option in the Configuration tab and links to download the backup agents for supported applications post the switch to VDP Advanced.

For more information on upgrading to VDP Advanced, refer to the vSphere *Data Protection 5.8 Administration Guide*.

Support for Multi-Tenancy

VDP replication features a new architecture to manage the replicated clients/backups individually. As all the data resides on the same appliance, this provides a logical separation of data from different users or tenants. Tenant accounts can be created on the replication target servers, which can be used to segregate the data. This is useful when dealing with a many-to-1 (fan-in) replication topology.

As an example, there can be many individual records or tenant accounts for a service provider, this new feature helps to manage the replicated clients/backups to provide each tenant its own flexibility to manage its own set of backups within a namespace.

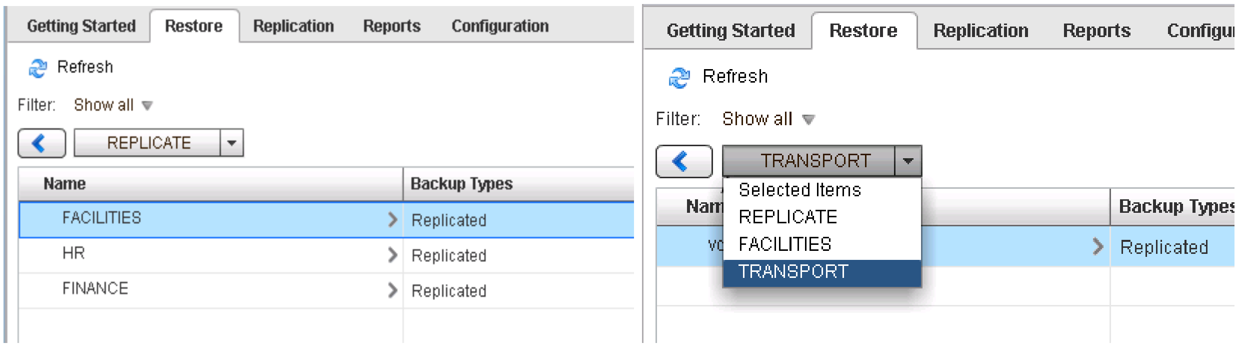
Data from multiple accounts is stored in the same appliance and is partitioned to provide better usability and allow multiple tenants to have their replicated backups show up in separate namespaces within the backup appliance.

VDP Advanced and VDP-RT provides the user an option to create their own tenant accounts under a single parent account. The user needs to provide tenant details and user credentials to create an account on the target host.

This multi-tenancy account can be created using a script provided on all VDP-RT 5.8.0.x appliances. The script is titled as ‘create_av_domain.rb’. Source server users can use these account details on the 'Destination' page of replication wizard using the 'Path' field to provide that details for tenant location. All the replication clients/backups from the source will get stored inside the tenant account.
All the tenant names will be created on the target appliance under the /REPLICATE domain by default.

For more information on the multi-tenancy support for replication and instructions on how to run the multi-tenancy script, refer to the vSphere *Data Protection 5.8 Administration Guide*.

Above screenshot shows specifying the Path after a tenant node is created



Name	Backup Types
FACILITIES	Replicated
HR	Replicated
FINANCE	Replicated

Nam	Backup Types
vc	Replicated

Above screenshots show the REPLICATE link with the 3 tenant domains created namely FACILITIES, HR, FINANCE. TRANSPORT is a sub tenant under FACILITIES.

Best practices for VDP-RT

Consider the following recommendations while selecting the destination target

- Ensure that the VDP Advanced or VDP-RT target appliance is up and running with a valid IP address, gateway and subnet mask.

- Ensure that there is a DNS record present for both the IP address and FQDN of the appliance (forward and reverse lookup enabled).
- Do not change the Port 29000 as this ensures encrypted mode of replication from source to target.
- Use the Verify Authentication button to validate the target appliance during replication job creation.
- Ensure that every replication job has a valid retention period.
- VDP-RT has a preconfigured user account called “repluser” which is used for configuring and running replication. The password of this user account is the same as the appliance password. For all replication activities in VDP-RT appliance, “repluser” account is recommended for configuring replication if using in a single customer or organization environment. If using VDP replication with multi-tenancy enabled, then it is recommended to use the respective username and password associated with the account created using the create_av_domain.rb script.
- It is recommended to keep the source and target appliances on separate vSphere hosts and different vCenter Server instances. This is to avoid single point of failure for the replication destination site.
- It is recommended to schedule backup jobs early in the backup window and schedule replication jobs later in the backup window. Only completed client backups are eligible for replication, so ensure that scheduled replications occur during periods of low backup activity.
- If the VDP-RT password is changed in the future then one needs to edit the replication job and reconfigure the destination with the new password.
- Ensure that time is synchronized across all VDP appliances, vCenter Server, and vSphere hosts.
- Keep a note on all the events, logs and alert messages shown in both the source and target appliance.
- Create multi-tenant user accounts for better segregation of replicated backups to their respective company and department in the target appliance.
- If using the fan-in replication topology, ensure that the target VDP-RT appliance is properly sized in terms of capacity.
- Monitor the capacity usage on the target appliance and use the VDP disk expansion feature to expand the storage to the required capacity when the target appliance reaches close to 80% used capacity. In case of Data Domain at both the source and the target of replication, the best practice is to limit the Data Domain capacity usage to 80%.

Limitations of VDP-RT

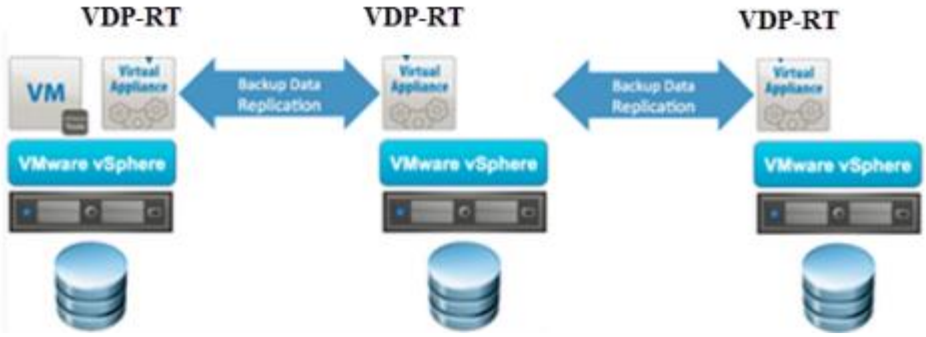
- Backup functionality is not available in VDP-RT.
- Automatic Backup verification (ABV) feature is not supported.
- External Proxy feature is not supported.

- User cannot change the identity of a VDP-RT appliance to VDP or VDP Advanced after deployment.
- Backups can only restored as new. Restore to original location is not supported for replicated backup data.
- FLR is not supported from VDP-RT.
- Emergency Restore is not supported for application level backup data.
- Backup data generated during a currently running backup job at source will not be included in the replication job in progress. The data will be part of the subsequent replication job.

Use cases for deploying replication target

1. In an environment containing hundreds of virtual machines, an important part of the overall backup strategy is to protect the data that is stored in VDP Advanced appliance and ensuring that critical backups can be recovered in case of disaster. Using VDP-RT appliance in a secondary site as a replication target for all the critical data can enable the backup administrator to have a secondary copy of the backup data which is useful incase the primary site goes down.

2. VDP-RT replicated backups can be replicated to multiple levels, i.e. Backup can be replicated from VDP-RT to target VDP-RT and then again to another target VDP-RT i.e. A->B->C-> etc. There is support for multi-hop replication policies with the ability to define a distinct policy at each hop. This will ensure longer retention policies get applied at each hop and also multiple backups are available for restore from different data centers during disaster.
   Example: User has all daily backups on the appliance A (VDP Advanced) and chooses to have all the backups replicated to appliance B (VDP-RT). User can define another replication policy for a tertiary site appliance C (VDP-RT) in order to provide another tier of protection.

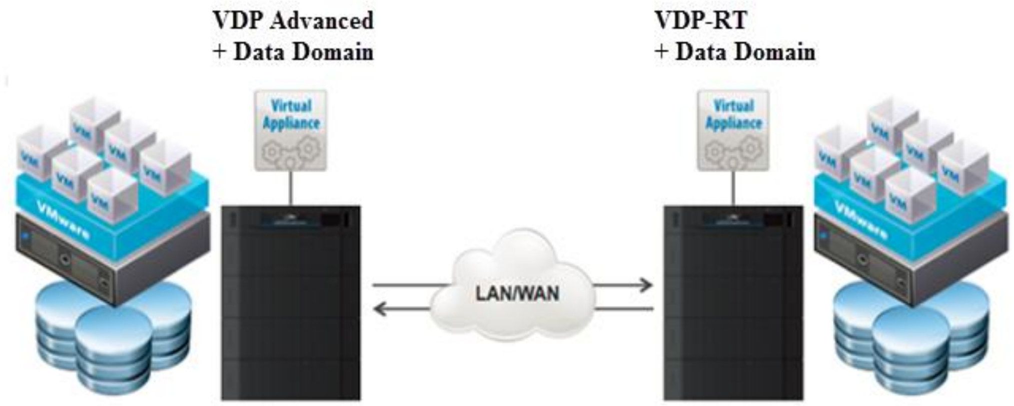


3. VDP-RT replicated backups can have a longer retention policy as compared to the original backup data. Since VDP uses unique and most storage-efficient deduplication capability, the storage requirement for the offsite replica is very minimal.
   Example: Consider the scenario where the source appliance can only have a retention policy of 30 days for all local backups. The source appliance has replication configured to a VDP

Replication Target. The replicated backup data retention policy can be set to following longer retention periods: Weekly for 24 weeks, Monthly for 12 months. Yearly for 2 years.

4. Consider an environment with Exchange, SQL Server, and SharePoint application databases protected by VDP Advanced. The backup data can be replicated to remotely located VDP-RT without any need to procure another VDP Advanced license. These replicated backups can then be restored in case of disaster and will provide another tier of protection for the applications.

5. A VDP-RT appliance attached with Data Domain system can be used to replicate the backup data from a VDP Advanced appliance attached with Data Domain system. Note that if backup data in the source appliance is stored on a Data Domain system then the target appliance for replication should also have a Data Domain system configured.



Conclusion

vSphere Data Protection Replication Target identity (VDP-RT) is a unique capability in VDP which provides a simple to deploy, low cost solution for replicating VDP Advanced backup data to a secondary site. As demonstrated in the topology overview, VDP-RT enables multiple topologies for replication, which provides multiple layers of protection for critical data. The use cases mentioned above validate that safeguarding critical data with offsite protection can be achieved very easily using VDP-RT appliances.

Glossary

VDP: vSphere Data Protection

VDP-RT: vSphere Data Protection Replication Target

VDPA: vSphere Data Protection Advanced

VM: Virtual Machine

VC: Virtual Center

ABV: Automatic Backup verification

FLR: File Level Restore

DNS: Domain Name Server

FQDN: Fully Qualified Domain Name

VMDK: Virtual Machine Disk

WAN: Wide Area Network

LAN: Local Area Network

SSL: Secure Socket Layer